NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

THE USE OF TELEMETRY IN TACTICAL NETWORK MANAGEMENT

by

Lucious B. Morton

September, 1994

Thesis Advisor: Lou Stevens
Co-Advisor: C. Thomas Wu

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503

1 AGENCY USE ONLY *(Leave blank)*	2 REPORT DATE September 1994	3 REPORT TYPE AND DATES COVERED Master Thesis

4 TITLE AND SUBTITLE THE USE OF TELEMETRY IN TACTICAL NETWORK MANAGEMENT (U)	5 FUNDING NUMBERS
6 AUTHOR(S) Morton, Lucious B	
7 PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000	8 PERFORMING ORGANIZATION REPORT NUMBER
9 SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10 SPONSORING/MONITORING AGENCY REPORT NUMBER

11 SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U S Government

12a DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited	12b DISTRIBUTION CODE A

13 ABSTRACT *(maximum 200 words)*
This thesis addresses the issue of reporting the real-time status of equipment in a tactical telephone system. The U.S. Army is developing a system called the Integrated System Control to manage all tactical communication networks. However, this system does not provide the network managers with a rapid and efficient tool for identifying and diagnosing network outages based on equipment failure. The current semi-manual method of reporting system residuals and failures allows for erroneous and delayed information that often leads to extensive troubleshooting procedures. The approach was to detemine if the tactical transmission assemblages can generate telemetry messages that contain the real-time status of the system's components. These messages would be routed through the tactical network to a centralized nodal control element and processed as status information to the network manager. We conclude that it is possible for military signal equipment to generate raw data pertaining to the "health and welfare" of a tactical network. A recommendation is given for processing this telemetry data into a computer using a Windows environment. This allows the network manager to monitor alarms from all transmission assemblages and perform queries to quickly determine the cause of system failures.

14 SUBJECT TERMS Telemetry, Digital Group Multiplex, Area Common User System, Integrated System Control, Network Management	15 NUMBER OF PAGES 62
	16 PRICE CODE

17 SECURITY CLASSIFICATION OF REPORT	18 SECURITY CLASSIFICATION OF THIS PAGE	19 SECURITY CLASSIFICATION OF ABSTRACT	20 LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev 2-89)
Prescribed by ANSI Std 239-18

Approved for public release; distribution is unlimited

THE USE OF TELEMETRY IN TACTICAL NETWORK MANAGEMENT

Lucious B. Morton
Captain, United States Army
B.S., South Carolina State University, 1985

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 1994

Author: ______________________________
Lucious B. Morton

Approved by: ______________________________
Lou Stevens, Thesis Advisor

____
C. Thomas Wu, Co-Advisor

____
Ted Lewis, Chairman
Department of Computer Science

ABSTRACT

This thesis addresses the issue of reporting the real-time status of equipment in a tactical telephone system. The U.S. Army is developing a system called the Integrated System Control to manage all tactical communication networks. However, this system does not provide the network managers with a rapid and efficient tool for identifying and diagnosing network outages based on equipment failure. The current semi-manual method for reporting system residuals and failures allows for erroneous and delayed information that often leads to extensive troubleshooting procedures.

The approach was to determine if the tactical transmission assemblages can generate telemetry messages that contain the real-time status of the system's components. These messages would be routed through the tactical network to a centralized nodal control element and processed as status information to the network manager.

We conclude that it is possible for military signal equipment to generate raw data pertaining to the "health and welfare" of a tactical network. A recommendation is given for processing this telemetry data into a computer using a Windows environment. This allows the network manager to monitor alarms from all transmission assemblages and perform queries to quickly determine the cause of system failures.

TABLE OF CONTENTS

I. INTRODUCTION 1

A. OBJECTIVE 1

B. TELEPHONE SYSTEM TERMINOLOGY 1

C. BACKGROUND INFORMATION 5

D. ORGANIZATION OF THESIS 7

II. NETWORK MODELING 9

A. TACTICAL EQUIPMENT OVERVIEW 9

1. Tactical Assemblages 9
2. Major Components 14

B. TELEPHONE SYSTEM MODEL 17

III. TELEMETRY REQUIREMENTS 21

A. HISTORICAL DATA 21

B. TELEMETRY FORMATTING 22

C. ORDERWIRE CONTROL UNIT CONCEPT 24

1. Two Kbps Operation 26
2. 16 Kbps Operation 27
3. 256 Kbps Operation 28

IV. IMPLEMENTATION TECHNIQUES 29

A. THE AIR FORCE APPROACH 29

1. Hardware 30
2. Software 31
3. Implementation 32

B. THE MITRE SOLUTION 33

1. Hardware 33
2. Software 34
3. Implementation 36

C. COMMERCIAL APPLICATIONS 39

V. RECOMMENDATIONS 41

A. RECOMMENDED APPROACH 41

1. Cost 41
2. Security 42
3. Expandability 43

B. SUGGESTIONS FOR FURTHER RESEARCH 44

VI. SUMMARY AND CONCLUSION 45
A. SUMMARY 45
B. CONCLUSION 45
APPENDIX A. ACRONYMS 47
APPENDIX B. TRANSMISSION TELEMETRY FORMAT 49
LIST OF REFERENCES 53
INITIAL DISTRIBUTION LIST 55

I. INTRODUCTION

A. OBJECTIVE

This thesis explores the use of an automated telemetry processing capability for reporting the real-time operational status of the Area Common User System, a battlefield telephone system that is part of the U.S. Army's tactical communications network. A management system should be capable of monitoring the network for changes in system status and failures. Through the integration of a software application, these changes are then displayed on a terminal at a central location, allowing the network manager to identify rapidly the cause of such changes.

This study has determined that it is possible through modifications on current equipment to ascertain the "health and welfare" of the network through the use of telemetry information generated by the transmission systems. The current semi-manual system of residual reporting is described and several methods for system improvement are discussed using both military and commercial technologies. A final recommendation is given of the most efficient approach to implementing telemetry capabilities to satisfy current applications of network management.

B. TELEPHONE SYSTEM TERMINOLOGY

Most homes today have telephones that we use as a source of communications. In many of these same homes, we can find computers and fax machines used as additional communicative gateways into the outside world. In order to communicate, these devices must interface with a *transmission system* that is responsible for getting our messages,

whether spoken or written, to the designated recipient(s). Our homes are tied into the transmission system via telephone lines that connect us to a *switching facility* operated by our local telephone company. These switching facilities are generally assigned to a geographical area and are responsible for determining the quickest, most efficient and available path for routing our telephone calls. All switching facilities across the country are connected to one another, either directly or indirectly, and together they make up a *communications network*. Depending upon the distance of your call, your switching facility may or may not have to interface with other such facilities. If you wish to call your neighbor down the street, this is considered a *local call* and only the switching facility assigned to your area is involved. If you call someone within your area code but you have to dial 1 before the number, this is known as a *long local call* and the assigned switching facility may have to route your call through another facility, depending on its size and capability. For calls made outside your area code, several switching facilities are required. The *transmission media* for the network is a combination of twisted pair wire, coaxial and fiber optic cables, microwave radios, and satellites.

Since the capacity of a transmission (switching) facility generally exceeds the requirements to transfer data between two devices, various techniques such as *multiplexing* are used to allocate the total capacity of a transmission medium among a number of users (customers). In this case, the actual transmission path is referred to as a *circuit* or *link*, and the portion of capacity dedicated to each pair of transmitter/receiver is referred to as a *channel*.[Ref. 1]

Each local telephone exchange has a *network management system* that is capable of reconfiguring the telephone system, monitoring its status, reacting to failures and overloads, and planning intelligently for future growth.

Now consider a telephone conversation. For two parties to engage in a conversation, one party must dial the number of the other, causing *signals* to be generated that result in the ringing of the called phone. The called party completes a connection by lifting the receiver. Once connected, the caller generates a message in the form of sound waves. The sound waves are converted by the telephone into electrical signals of the same frequency. These signals can be *analog* or *digital*. An analog signal is a continuously varying electromagnetic wave that may be propagated over a variety of media. A digital signal is a sequence of voltage pulses that may be transmitted over a wire medium.[Ref. 1]

When the caller or called person speaks, their message is defined as *data*. Data can also be viewed as analog or digital. Analog data take on the continuous values on some interval, such as the way our voices sound. Digital data take on discrete values, much the way computers talk to each other. Digital data can be represented by analog signals by use of a *modem* (modulator/demodulator). The modem converts a series of binary (two-valued) voltage pulses into an analog signal by encoding the digital data onto a carrier frequency. The resulting signal occupies a certain spectrum of frequency centered about the carrier and may be propagated across a medium suitable for that carrier. In an operation very similar to that performed by a modem, analog data can be represented by

digital signals. The device that performs this function for voice data is a *codec* (coder-decoder). In essence, the codec takes an analog signal that directly represents the voice data and approximates that signal by a bit stream. At the receiving end, the bit stream is used to reconstruct the analog data.[Ref. 1]

In terms of theory and connectivity, a military tactical communications network is very similar to a commercial telephone network. In order for soldiers to communicate on the battlefield, they still need routers, carriers, and multiplexers. Only these components must now be sturdy and mobile, and they are generally housed in an assemblage/shelter that is mounted on the back of tactical vehicles for transportability around the battlefield. Figure 1 is a pictorial display of a tactical communications shelter with vehicle.

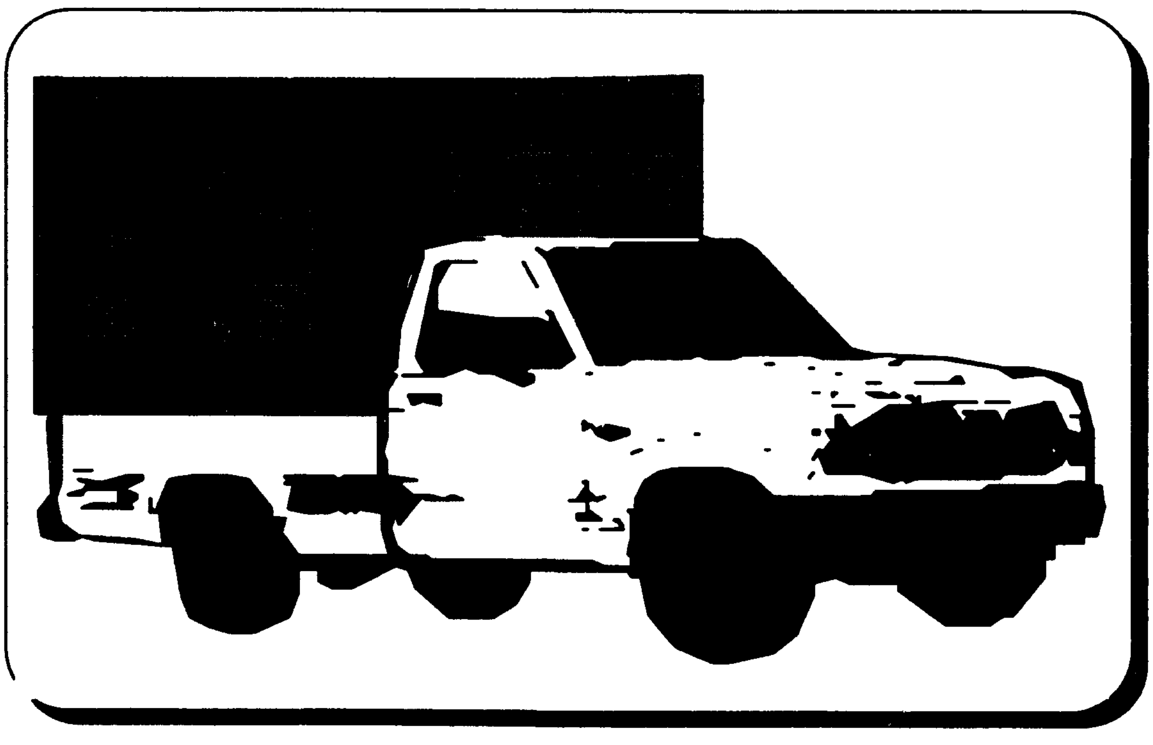

Figure 1: Tactical Communications Assemblage

Mobile switching facilities, commonly known as circuit and message switches, are being used for routing voice and hardcopy messages throughout the tactical network. Because time is mission critical, communicators rely heavily on microwave radios and satellite media to establish the backbone of the network with relay repeaters extending the distance between nodes (switching facilities). Cable and wire usage are generally confined to distances of 8 km (5 miles) or less.[Ref. 2]

C. BACKGROUND INFORMATION

During the 1970s and 1980s, the U.S. Army replaced most of its old tactical communications equipment that used analog technology with modern equipment utilizing digital technology. As a result, current tactical networks provide for secure digital voice and data communications capabilities as well as global positioning systems. However, only manual systems now exist for monitoring and reporting the operational status of the tactical networks. Realizing the need for a computerized network management capability, the U.S. Army Signal Corp is currently developing the Integrated System Control to manage all tactical communications networks. The system will automate the functions of wide area network management, network planning and engineering, battlefield frequency management, communications security management, and communication asset command and control for the three classes of communications systems. Table 1 contains the communications classes and their functions.[Ref. 3]

While the Integrated System Control will provide enhanced capabilities for network management, it does not address the issue of real-time tactical telephone system

monitoring and equipment status reporting as required in the Area Common User System. Without this capability, communications commanders still do not have a rapid and efficient tool for identifying and diagnosing system outages.

TABLE 1: ARMY COMMUNICATIONS CLASSES

COMMUNICATIONS CLASS	PROVIDES USER WITH
Area Common User System	Battlefield telephone system
Combat Net Radio	Secure single channel communications
Army Data Distribution System	Communications for tactical data systems

Signal Corp commanders and network managers still rely on the operators to identify system failures and to transmit accurately and effectively such information over LS-147 loudspeakers and FM radios. On the basis of such information supplied by the operators, managers must make rapid decisions as to the appropriate actions for system recovery. Options include switching to backup systems or allowing down-time for on-line troubleshooting procedures. The initial assessment of the cause for system failure is usually determined by the operators from alarm status indicators inside the communication shelters. These indicators set off a manual troubleshooting process that, as indicated in Table 2, can take a significant amount of time. In addition, there is a high probability that due to the reconfigurations required to implement the various equipment loopbacks, an

incorrect configuration may be left in place even after the original source of the problem has been identified and rectified [Ref. 4]. If these same alarm indicators can somehow be converted and transmitted in data form over the network and terminated inside the Communications System Control Element (CSCE) or a similar shelter, this would allow the senior leadership to have access to the same information as the operator inside the shelter. This concept of putting real-time information directly into the hands of people that make the decisions will vastly enhance communications support across the battlefield.

TABLE 2: TROUBLESHOOTING PROCESS

EVENTS	APPROXIMATE TIME	
	MIN	MAX
Customer report disruption of service	1 minute	30 minutes
Nodal managers validate loss of signal	1 minute	3 minutes
Troubleshooting techniques and recovery	12 minutes	60 minutes
TOTAL DOWNTIME PER FAILURE	~15 minutes	~90 minutes

D. ORGANIZATION OF THESIS

This thesis is divided into six chapters and two appendices. Chapter II provides an overview of a tactical communication nodal network and the transmission equipment utilized at theater level. Chapter III discusses telemetry requirements and the concept for installation of automated processing capabilities. Chapter IV presents several implementation methods for enhanced network management. A recommendation is given

in Chapter V on the most economical and efficient approach to providing real-time network residuals along with suggestions for further research. Chapter VI summarizes the study and looks to the future of tactical communications network management. The first appendix contains a listing of acronyms. The second appendix contains tables of the transmission telemetry format and protocol.

II. NETWORK MODELING

This chapter gives an overview of a tactical nodal network within the Area Common User System. It provides descriptions and roles of the communications assemblages and components utilized within such a network. A detailed communications example is presented to give the reader a better understanding of how the components interrelate and how complex the troubleshooting process can be when failures occur.

A. TACTICAL EQUIPMENT OVERVIEW

The Area Common User System is divided into two subsystems -- one that supports echelons above corps (EAC) units and one that supports echelons corps and below units. The EAC subsystem is supported by Digital Group Multiplex (DGM) equipment while the echelons corps and below subsystem is supported by Mobile Subscriber Equipment (MSE). Relatively speaking, the main differences between the two subsystems are the channel rates, circuit routing strategies, mobile subscriber support, and *International Consultative Committee on Telegraphy and Telephony* (CCITT) X.25 packet switching service. Therefore, this chapter will only focus on communications support at the EAC level.[Ref. 5]&[Ref. 6]

1. Tactical Assemblages

The DGM family of communications assemblages provide the physical path for *digital transmission groups* (DTGs). The term digital transmission group refers to a collection of full duplex channels that connect two nodes. These channels can be trunks, telephone loops, or data loops. Digital transmission groups originate from an AN/TTC-39

circuit switch and terminate either to another circuit switch, a telephone multiplexer device, or another type of terminating equipment. They can be transmitted over cable or radio links. Multiple digital transmission groups (known as *super groups*) can be multiplexed together and transmitted over links.[Ref. 2]

Trunks provide communication paths between different circuit switches. In almost all cases, trunks between circuit switches are a combination of cable and radio links. Cable links are used to connect equipment that is separated by a short distance that is 8 km (5 miles) or less. They are generally used to connect line-of-sight (LOS) radio shelters, a circuit switch to line-of-sight radio shelters, and circuit switches used in special configurations. Radio links greatly increase the distance between circuit switches, generally up to 40 km (25 miles).[Ref. 2]

The DGM assemblages also provide the capability to extend voice, data, and message service to customers that are not directly supported by a circuit switch. Five types of assemblages make up the DGM family. A typical nodal complement of these assemblages is depicted in Figure 2.[Ref. 4]

The TRC-173 is an ultra high frequency (UHF) LOS radio shelter used to extend the connectivity of the network through radio links. In the Area Common User System, the TRC-173 is primarily utilized as a radio or cable terminator, connected to a Remote Loop Group Multiplexer (RLGM) or a Remote Multiplexer Combiner (RMC) which multiplexes and demultiplexes four to eight full duplex telephone loops respectively. It can accommodate two supergroups and can operate as a split terminal, with radio and

cable systems simultaneously. In addition, the TRC-173 also has the capability to function as a relay. The planning range for the TRC-173 is 40 km (25 miles) for radio and 64 km (40 miles) for cable systems.[Ref. 2]

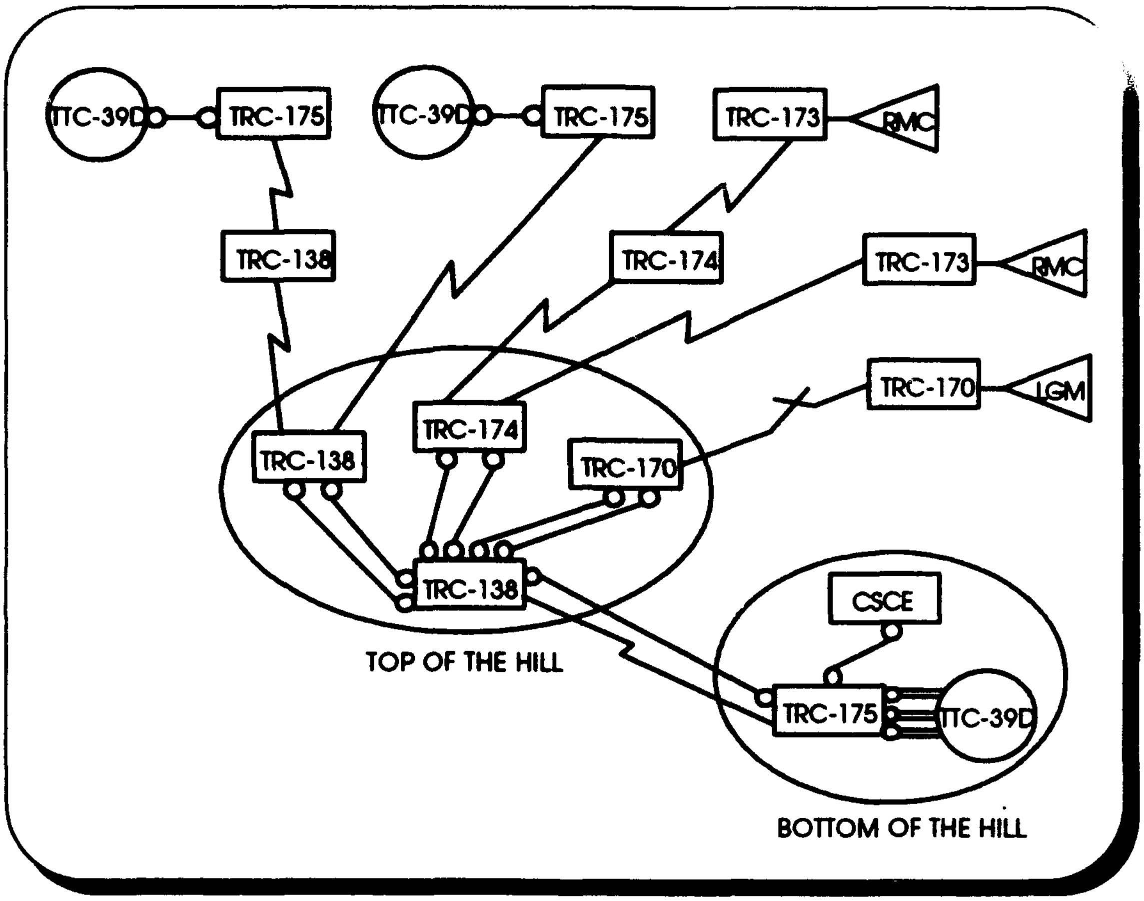

Figure 2: EAC Nodal Transmission Network

The TRC-174 is also an UHF LOS radio repeater. The TRC-174 is capable of functioning as a radio-to-radio relay, a cable-to-radio relay, or a cable-to-cable relay. The relay can be between two switches or between a switch and a TRC-173 radio terminal that terminates a DTG from the switch. The TRC-174 can accommodate up to three

supergroups when deployed at the top-of-the-hill. The planning range for this assemblage is also 40 km (25 miles) for radio and 64 km (40 miles) for cable systems.[Ref. 2]

The TRC-170 is a tropospheric scatter radio terminal that generally provides extended digital trunking between major nodes. The TRC-170 is similar to the TRC-173 in that it can terminate a DTG from a switch and can use internal multiplexers to break out the subscriber channels or connect to a Loop Group Multiplexer (LGM). The planning range for a TRC-170 is 100 to 150 miles, depending on which version (V1/V2/V3) is in use. Two TRC-170s are often used at one tactical relay site for range extension.[Ref. 2]

The TRC-138 is a super high frequency (SHF) LOS radio or cable repeater that is designed to combine all of the transmission links coming into a node at the "top-of-the-hill". The concept of the top-of-the-hill of a node is to displace the assemblages that emit a radio frequency signature away from the circuit switch at the "bottom-of-the-hill". The combined transmission links (up to 12 links) comprise a master group that is transmitted to a TRC-175 SHF LOS radio terminal at the bottom-of-the-hill. The individual transmission links traversing the master group are broken back down into individual groups and cabled to the circuit switch. The link between the top-of-the-hill TRC-138 and the bottom-of-the-hill TRC-175 can be installed over tactical pulse code modulation (PCM) cable, fiber optic cable, or a short-range wide-band radio (SRWBR) system. When used as a radio terminal, the planning range of the TRC-138 and TRC-175 are 40 km (25 miles), however, in a SRWBR configuration they are restricted to 8 km (5 miles) due to the high speed data rates.[Ref. 2]&[Ref. 4]

Each DGM communications shelter is typically operated by a 3-man crew consisting of a team chief and two team members. They are responsible for the installation, operation, and maintenance of the transmission system(s) assigned during a tactical operation. This also includes 24-hour surveillance of on-line equipment and hourly reporting of system residuals/status to the network managers at the company level. Company commanders, along with their operations personnel (network managers), are co-located with the circuit switch at the bottom of the hill inside the CSCE.

The TTC-39 circuit switches provide the capability to monitor the DTG overlay to the tactical transmission network. It does so by monitoring the status of the DTGs that it is terminating from other switches or from remote multiplexing equipment. Referring to the nodal view of the tactical transmission network in Figure 2, the circuit switch would provide a level of detail of the status of the network as indicated in Figure 3. The dashed

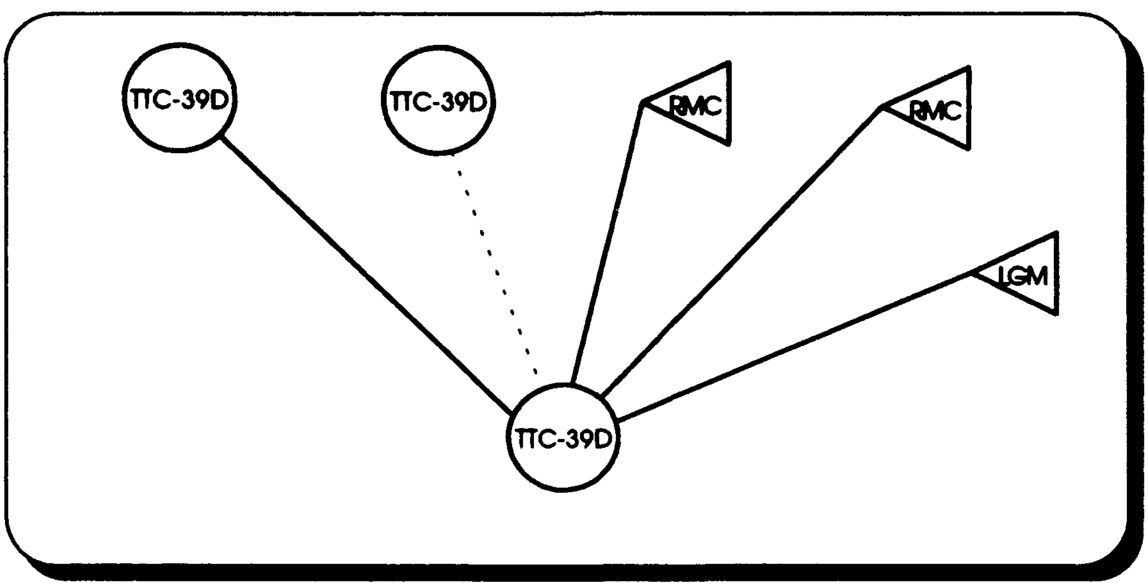

Figure 3: Status of the DTG Network

line presents a DTG that is out of service between the two switches. The CSCE provides a capability similar to the TTC-39 circuit switch to monitor the DTG overlay to the tactical transmission network. In fact, the CSCE monitors the alarms of the TTC-39 circuit switch. However, the CSCE currently do not have the capability to monitor individual systems and the several components that make up these systems.[Ref. 4]

2. Major Components

The DGM equipment is a family of digital loop and group multiplexers, cable driver modems, and pulse restorers that are responsible for performing the basic signaling process. There are several different digital signals used with the DGM equipment. These vary depending on the particular piece of equipment and its intended application. The characteristics of each type of signal are briefly described below:

- Conditioned Diphase Group Signals: These are unbalanced, four-wire, 3 Volts peak-to-peak, conditioned diphase signals transmitted over Pulse Code Modulation (PCM) cable. The interface is normally used on the line (or cable) side of modems. Data rates can range from 72 kbps to 4608 kbps.

- Dipulse Group Signals: These are unbalanced, four-wire, 1.8 Volts peak-to-peak, dipulse signals at a constant 2.304 Mbps rate. They are also transmitted over PCM cable with a maximum distance of 1.6 km (1 mile).

- Nonreturn-to-zero (NRZ) Signals: These are balanced, four-wire, +/- 3 Volts signals transmitted over RG-108 cable. These signals are used to interconnect DGM equipment within a shelter.

Although there are many components that play a part in tactical point-to-point communication, the major items are as follows.

- Group MODEM (GM)
- Low and High Speed Cable Driver MODEMS (LSCDM and HSCDM)
- Loop Group Multiplexer (LGM)
- Trunk Group Multiplexer (TGM)
- Master Group Multiplexer (MGM)
- Trunk Encryption Device (TED)
- Radio MODEM (RM)

The purpose of the Group MODEM is to provide an interface from a PCM cable link to the DGM shelter. It converts a cable link signal to a NRZ signal and a NRZ signal into either a conditioned diphase or dipulse signal. There are four cable connection slots per GM and there are two GMs per shelter.[Ref. 2]

The Low and High Speed Cable Driver Modems (LSCDM and HSCDM) are used on both ends of a repeated PCM cable transmission system to switch the signal from NRZ to unbalanced conditioned diphase. They provide signal and power for the unattended Low and High Speed Pulse Restorers (LSPR and HSPR), which retime and regenerate the group signals. LSCDM systems may be up to 64 km (40 miles) in length while HSCDM systems are 8 km (5 miles) or less.[Ref. 2]

The Loop Group Multiplexer (LGM) is a shelter mounted component that multiplexes up to sixteen 32 kbps subscriber loops (telephones) into a single group. A

switch on the loop modem card allows the LGM to provide power to digital telephones a maximum of 3.2 km (2 miles) away.[Ref. 2]

The Trunk Group Multiplexer (TGM) is also a shelter mounted component that multiplexes and demultiplexes up to four NRZ signals from the GM into a supergroup. The group inputs can be 72-2304 kbps and the TGM output can be 128-4608 kbps. There is a total of two TGMs per shelter.[Ref. 2]

The Master Group Multiplexer (MGM) is a shelter mounted second level multiplexer that combines up to 12 NRZ groups or supergroups at rates of 72-4915.2 kbps and two 16 kbps NRZ signals into a single serial bit interleaved NRZ mastergroup. It can operate at rates of 9.36 Mbps or 18.72 Mbps and is generally used in the SRWBR configuration.[Ref. 2]

A Trunk Encryption Device (TED) can be connected to each TGM to encrypt and decrypt the signals (supergroups) passing through it. It provides the means for double encryption between the assemblages only.

The Radio MODEM is used to convert the NRZ signal from the TED into a radio binary signal and vice versa. There are three MODEM slots within one RM unit. The microwave radio unit then transmits/receives the radio binary signal to/from a distant-end assemblage.[Ref. 2]

Every DGM assemblage does not contain all of the previously discussed components. These components are assigned based on the roles and functions of the assemblage within the network. However, it is very important to note that each of these

components contains overhead channels that can be utilized for timing, framing, and telemetry.

B. TELEPHONE SYSTEM MODEL

To complete an end-to-end telephone connection, several assemblages and components discussed above will be required. Figure 4 illustrates how telephone service is provided through a portion of the network. This example displays the signal path from a telephone at Site 1 to another telephone at Site 3. There are two digital transmission groups (DTGs), both originating at the circuit switch (CS). DTG 1 and DTG 2 provide local site telephone service to RMC 1 and RMC 2 respectively.

There are three line-of-sight (LOS) radio connections: L1, L2, and L3. The five cable connections (C1, C2, C3, C4, C5) are generally made with PCM CX-11230 cable. Telephones are connected to the RMCs via a four-wire interface such as WF-16 wire.

A telephone call from RMC 1 to RMC 2 would be considered a long local call since both the calling and called telephones are receiving service for the same circuit switch. Channels are multiplexed at RMC 1 and sent to the CS. The CS encrypts the signal at the TED and straps it onto DTG 2 which goes to the TRC-175. The MGM will multiplex DTG 2 with any other DTGs it receives from the CS and the signal is transmitted to the top-of-the-hill by the GRC-222 radio which has an internal radio modem that provides the interface between the radio and the NRZ signal. It is important to note here that a cable system is typically installed as backup to the radio system. This is necessary because every system (up to 12 max) at the top-of-the-hill is being multiplexed

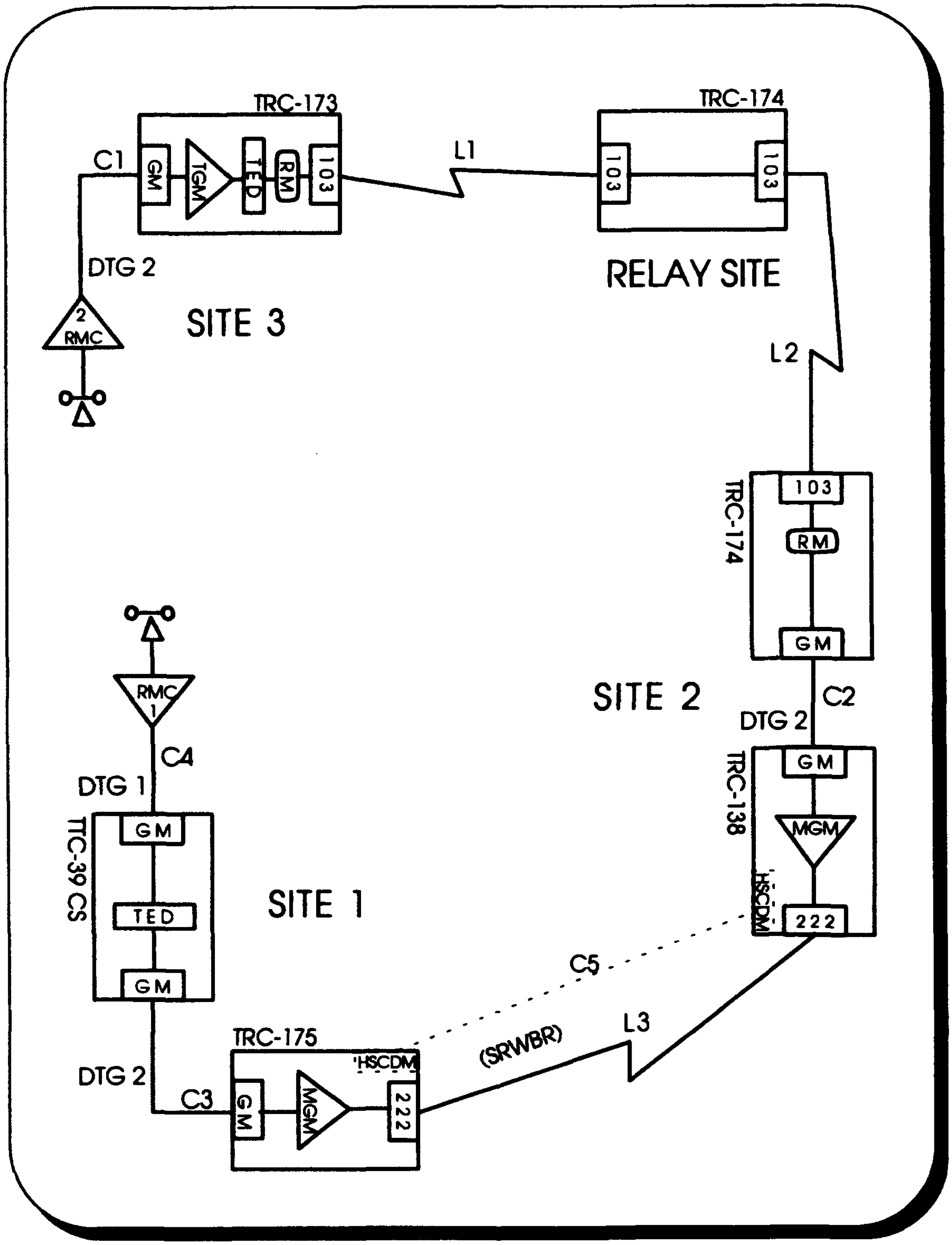

Figure 4: Telephone Service Example

over this transmission. If the SRWBR system fails, all subscribers being supported by the CS will lose telephone service. It is critical to have a rapid backup plan. The MGM in the TRC-138 demultiplexes all the DTGs and sends DTG 2 to the TRC-174 via cable. Since both assemblages are equipped with GMs, this is possible. The TRC-174 then relays the signal to another TRC-174 which relays the signal to the distant-end TRC-173. Since the TRC-174 at the relay site is acting as a repeater, only the GRC-103 radios are utilized. At the TRC-173, the supergroup is decrypted and demultiplexed by the TED and TGM respectively, and DTG 2 is sent to the RMC 2 that demultiplexes the DTG into eight individual channels. The TGM can accept four DTGs, allowing the TRC-173 to interface with four RMCs (32 subscribers). In addition, each RMC can connect to another RMC or RLGM, providing telephone service for 64 subscribers.

In summary, a telephone call from Site 1 to Site 3 utilizes the following components:

- GM -- six each
- TGM -- one each
- MGM -- two each
- RM -- four each (two internal)
- TED -- two each
- Radio -- six each
- RMC -- two each
- HSCDM -- two each (backup)

A failure in any one of these components (to include the cable system with Pulse Restorers) will cause the subscribers to be without communication support. For this reason, it is important for network managers to identify quickly the source of failure. Because the system is dependent upon timing and framing techniques for synchronization, a failure of one component will cause alarms to be triggered in all assemblages, making it difficult to identify manually the faulty components.

When the system fails, troubleshooting procedures begin at the CS, which will put RMC 1 and the TRC-175 into system loopbacks. This allows the equipment to check the signal path to the switch. If these loopbacks are error-free, the CS will continue to put the next assemblage in the link in a loopback until the faulty component is found or until it reaches the end of the path at RMC 2. This procedure accounts for the lengthy downtime discussed in Table 2 of Chapter 1.

III. TELEMETRY REQUIREMENTS

The objective of this chapter is to discuss the concept of generating telemetry data within a tactical network. Telemetry is defined as a science or process of using an electrical apparatus for measuring a quantity (as pressure, speed, or temperature), transmitting the result by radio to a distant station, and there indicating or recording the quantity measured [Ref. 7]. From a network perspective, it is the use of telecommunications for automatically indicating or recording measurements at a distance from the measuring instrument. Consequently, telemetry data consists of status information and subcomponent alarms from the communications assemblages in a tactical transmission network.

A. HISTORICAL DATA

During the research phase of this thesis, it was discovered that a telemetry processing capability was initially included in the design aspects of the DGM specifications in 1976. The concept was a compromise between the user requirement to know instantaneously the status of all transmission equipment and the available microprocessor technology of the mid-1970s. All telemetry information was to be transmitted to the to-be-developed nodal control processor for use by the technical controllers. Equipment status would be reported over data orderwires by telemetry, teletype and processor-to-processor links. Message format, synchronization content and handshaking required for telemetry reports and processor interchange would have to be established as would the signaling interfaces for analog and digital voice orderwire circuits.

In the late 1970s, the Army developed the Orderwire Control Unit (OCU), a current component of all DGM assemblages. One of the functions of the OCU was to generate the telemetry information for each assemblage. The assemblages were designed to house the OCU and at least one Dedicated Loop Encryption Device (DLED) to encrypt the telemetry messages. However, the telemetry concept could not be tested during operational testing of the DGM system due to lack of nodal control processors to process the telemetry information.

In 1982, the Army decided to abort its nodal control management program due to funding and this halted the effort to effectively develop telemetry processing. The DGM assemblages were fielded to tactical units in the late 1980s without such a vital capability. Consequently, during the development of the current AN/TTC-39 circuit switches and CSCE programs, telemetry was not considered to be one of the minimum essential technical control functions due to networking and security issues.

B. TELEMETRY FORMATTING

Using the theoretical layout of a tactical transmission network as viewed in Chapter 2, it is now appropriate to discuss the concept of telemetry within this network. Figure 5 depicts a standard telemetry message format. The telemetry data is formatted into a block oriented structure with each block consisting of 20 characters. Specific fields within each block uniquely identify the origin of the telemetry data, i.e., the station identifier (ID). The station ID consists of a letter followed by two numeric characters. The initial letter of the station ID also serves to identify which type of shelter is reporting

the telemetry data. Subsequent fields reveal the status of the assemblage: P, indicating all is well; K, indicating a bit error rate (BER) threshold has been exceeded; and finally E, indicating that there are errors to report.[Ref. 4]

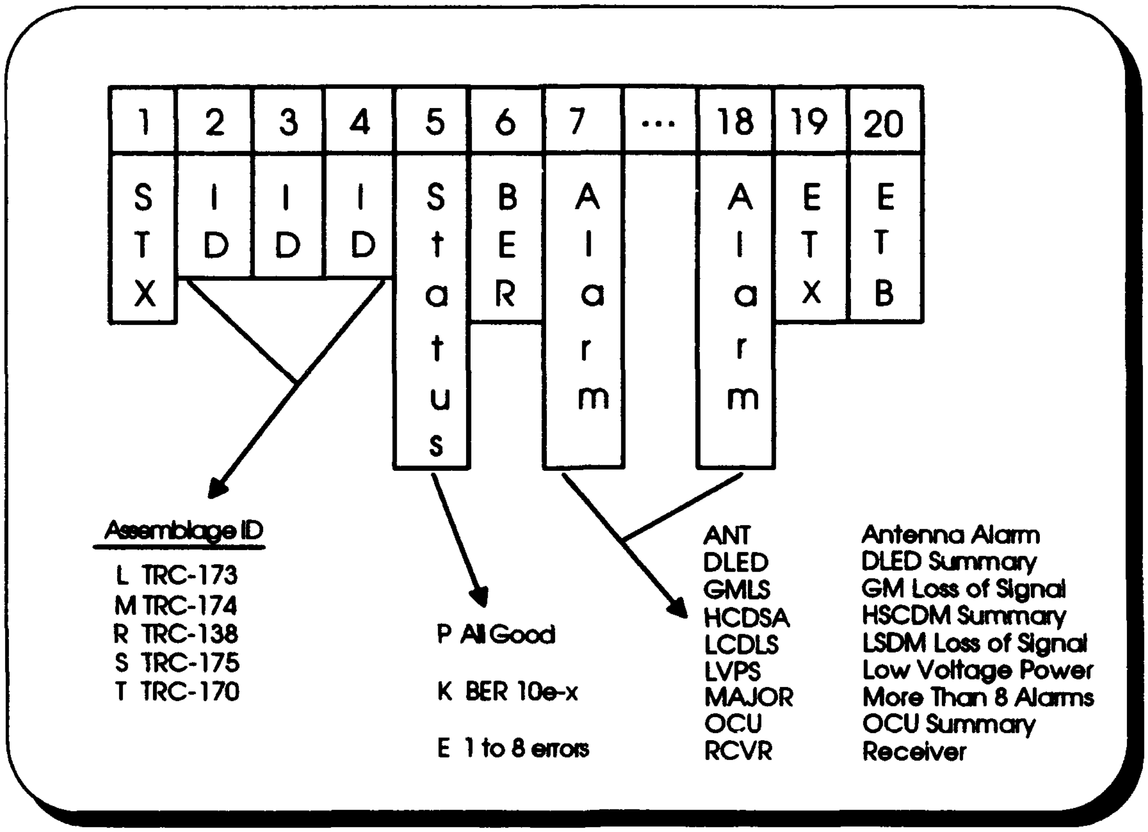

Figure 5: Telemetry Message Format

If the assemblage is reporting errors, then the specific alarms would follow within the message. Two alarms can be reported per block with up to four blocks composing a valid assemblage message. Therefore, any assemblage can report up to a total of eight alarms. Any assemblage with more than eight alarms would report the unique code word of "MAJOR". In general, the alarms can be categorized into summary alarms and loss of signal alarms for subcomponents such as the modems, receivers, transmitters, and

multiplexers. A table of the transmission telemetry format and protocol with detailed explanations of the 20-character block is provided in Appendix 2.[Ref. 4]

C. ORDERWIRE CONTROL UNIT (OCU) CONCEPT

Although the Army failed to realize the significance of the nodal control facility, modifications made to the orderwire control units (OCUs) in the mid 1980's has made it possible to deliver telemetry. The OCU in each DGM assemblage control the generation and transmission of telemetry messages. Each OCU is composed of 3 separate entities as follows:

- Data Orderwire (DOW)
- Digital Voice Orderwire (DVOW)
- Analog Voice Orderwire (AVOW)

The data orderwire (DOW) system is physically responsible for transporting telemetry data throughout the network. The digital voice orderwire (DVOW) and the analog voice orderwire (AVOW) systems facilitate the installation and troubleshooting of a transmission system. Each system is capable of generating a telemetry stream structured in the block-oriented format previously discussed. The DOW and DVOW streams are transmitted out-of-band. The AVOW is frequency multiplexed as a subcarrier to the transmission system. The AVOW is generally the first system that is available to the operators when installing a system. However, it is not extensively used after initial system installation. The DVOW is used more extensively and provides the capability to set 'ring codes' that can signal a specific assemblage within the transmission link to answer the

DVOW. As such, the DVOW is used most often to manually direct and coordinate troubleshooting activities.[Ref. 4]

There are four types of OCUs, as depicted in TABLE 3. The OCU-I, OCU-II, and TOCU have a telemetry controller that monitors contact relays in the subcomponents of the assemblage. These contact relays open and close dependent on whether the component is experiencing an alarm. Based on the status of these relays, a continuous 150 bit per second (bps) telemetry data stream is generated which contains the local assemblage status information.[Ref. 4]

TABLE 3: Types of Orderwire Control Units

TYPE	LOCATION	COMMENTS
OCU-I	UHF	Can demultiplex 3 separate 2 kbps DOWs
OCU-II	SHF	Contains Data Channel Multiplexers (DCM)
OCU-III	CSCE	Can not support 2 kbps operation
TOCU	TROPO	Can report Bit Error Rate (BER)

The DOW system is composed of three distinct multiplexing hierarchies: operation at the two kbps level, the 16 kbps level, and finally at a level of 256 kbps.

1. Two Kbps Operation

Each orderwire control unit has a telemetry decombiner and combiner (TD and TC) that respectively character demultiplex and multiplex 13 separate 150 bps channels into a two kbps DOW. If the assemblage is the last (or first, depending on the point of view) one in the transmission link, then there is no two kbps DOW to demultiplex. In this situation, the shelter locally generates the two kbps DOW, substituting fill data (hex FF) for the empty channels. An operator-set dual-in-line package (DIP) switch determines which channel assemblage's local telemetry data will be inserted onto. This resulting two kbps DOW transmitted out-of-band over the transmission system to the adjacent transmission assemblage towards the node. At the adjacent assemblage, the process repeats itself, with exception that the next assemblage character demultiplexes the incoming DOW into 13 individual channels, one of which is not empty. This assemblage's local telemetry data is then inserted onto the designated empty channel.[Ref. 4]

All the OCUs, with the exception of the OCU-III, support two kbps telemetry operation. Each supports the selection of a station ID for the assemblage, the selection of one of 13 channels out of the two kbps DOW for its local telemetry data, and the demultiplexing and multiplexing of the two kbps DOW. The OCU-I found within the UHF LOS assemblages has the added flexibility of being able to decombine (demultiplex) either a single two kbps DOW or three separate two kbps DOWs. If it is configured to decombine three, then the first four channels of DOWs one through three make up channels 1 through 12 respectively of the recombined two kbps DOW. In this case, the

local shelter's telemetry data should be inserted onto channel 13 in order not to overwrite one of the incoming 12 channels.[Ref. 4]

The TOCU within the TRC-170 also has the capability to report the BER of the radio link. If there are no alarms, yet the BER has deteriorated to between 10^{-3} and 10^{-5}, then a status character of "K" is generated. A "K" indicates that the radio link is in a marginal status.

2. 16 Kbps Operation

Once all the transmission links and their corresponding two kbps DOWs reach the top-of-the-hill, the mission groups are combined into a master group. All the two kbps DOWs appear at the patch panel of the TRC-138 where they are individually patched to one of two data channel multiplexers (DCMs). The DCM, which is found only within the OCU-II, has the capability to bit multiplex the individual two kbps DOWs into a 16 kbps telemetry data stream. Up to seven two kbps DOWs can be bit multiplexed by the DCM in the OCU-II. The eighth input to the DCM consists of a binary overhead framing sequence of 0001001. Since there are two DCMs, the OCU-II can process two of these 16 kbps telemetry data streams.[Ref. 4]

Now that all the telemetry data is present within one or two 16 kbps telemetry data streams at the top-of-the-hill, the data must be further processed for transmission to the bottom-of-the-hill. This is done by multiplexing the 16 kbps telemetry data streams with other 16 kbps digital voice orderwires (DVOWs) into a 256 kbps digital group.

3. 256 Kbps Operation

The DVOW multiplexer in the OCU-II multiplexes the two 16 kbps telemetry data streams along with up to 12 other 16 kbps DVOWs into a 256 kbps digital group. This 256 kbps digital group is then multiplexed by a master group multiplexer (MGM) into the master group that is transmitted from the top-of-the-hill down to the bottom-of-the-hill. At the bottom-of-the-hill the 256 kbps digital group is demultiplexed from the master group and then directed to the OCU-III in the nodal CSCE. A DVOW multiplexer in the OCU-III then breaks out individual DVOWs and telemetry data streams.[Ref. 4]

The ability to deliver the telemetry data to a currently unused port on the rear of the OCU III in the nodal CSCE does exist. Unfortunately, there is not an existing capability to monitor and exploit this useful source of data. Two issues must be addressed:

- How to get the raw telemetry data into a CSCE or equivalent processor.
- How to translate the raw data into information that network managers can use.

IV. IMPLEMENTATION TECHNIQUES

This chapter presents current methods for gathering raw telemetry data and converting it into vital information for network managers. It discusses the Air Force's network management system and a prototype system developed by the MITRE corporation. The chapter concludes with an overview of commercial off-the-shelf equipment that enhances network management.

A. THE AIR FORCE APPROACH

In the 1970s, the Air Force was part of the joint military working group for development of digital communications. When the Army aborted its nodal management program, the Air Force continued to press forward and fielded the AN/TSQ-111 assemblage, commonly known as the Communications Nodal Control Element (CNCE). This shelter provides the means by which communications resources at a node are assigned, monitored, controlled, and managed for users of the tactical communications system. The CNCE was designed to improve the performance of a communications network by providing timely information to a CNCE controller. Information processing and display capabilities are integrated with existing system elements to improve the correlation of relevant information. These capabilities also improve the exchange, handling, and presentation of data required for making decisions pertaining to the status of a transmission network.[Ref. 8]

The CNCE can perform its assigned functions in an environment consisting of a hybrid mixture of analog and digital transmission, circuit switching, and store-and-forward

(S&F) message switching equipment. The CNCE is also designed to provide the means for an orderly transition to a capability that will allow it to perform the assigned functions in future all-digital systems.

The functions of the CNCE are twofold: (1), it provides the interface between transmission facilities and users, and (2), the CNCE provides the capability to manage communications resources at a node. The CNCE provides the means for carrying out the following functions:

- Implement communication orders at the communications node and coordinate necessary actions required for the timely and responsive installation and restoration of communication circuits originating at, terminating within, or routed through the communications node.

- Report nodal communications equipment alarms and maintain those records essential for planning and control of all the elements in the node.

- Analyze critical transmission parameters from monitoring activities to identify and provide warning of circuit/system degradation or failure within the communication network in the timely manner required for rapid fault isolation and corrective action.

- Process, evaluate, store, edit, and display data relative to transmission standards, system/circuit quality and status, and required reports.[Ref. 8]

1. Hardware

The CNCE provides the network manager with the console and peripherals necessary to perform the required functions. The data processing equipment includes the

AN/UYK-20 CP-1303A/T computer with 64K 16-bit words of memory. It has a fixed hard disk with 250M of memory. The manager monitors activity on the network using an 80 character by 50 line Visual Display Unit (VDU) and a Hard Copy Printer is provided for paper logs, along with keyboard and lightpen. Additional interfaces are provided to permit the CNCE management functions to be performed external to the shelter at a remote location.

2. Software

The menu-driven CNCE software includes both automatic and Controller-initiated tests that monitor the CNCE and external nodal equipment under its control, and provides electronic patching and multiplexing of digital circuits. Automated processing reduces the data and presents it to the manager through advisories and displays. Through software, the CNCE is able to process data in assisting the network manager in:

- Determining the cause of group transmission impairment, i.e., loss of synchronization, loss of signal or BER exceeding threshold.
- Isolating the equipment and/or the portion of the system responsible for group transmission degradation.
- Identifying failed transmission equipment located either internal or external to the CNCE.
- Maintaining a list of transmission equipment in a state of failure.

A data set of the last received inputs containing fault information is maintained to provide a current transmission network status display. The display is automatically updated as fault conditions change.[Ref. 8]

3. Implementation

Digital circuits are connected to the CNCE Signal Processing Facility (SPF) through the Primary Patch Panel (PPP), a modular facility for use with circuits passing through or terminating in the CNCE. DTGs are interconnected via the patch panel and terminated on the appropriate GM and/or cable driver modem to support connectivity to several different types of transmission media and/or nodal equipment. The CNCE processes digital trunks groups that employ the nominal 16 or 32 kbps digital channel rates.[Ref. 8]

The CNCE accepts the following inputs for satisfying the nodal diagnostics function which provides the capability to process data to assist the network manager:

- Transmission status data in ASCII format.
- Automatic Digital Tester (ADT) group BER and DGM performance data.
- Channel Reassignment Function (CRF) status data.

The CNCE is capable of accepting the telemetry data generated by the OCUs within the DGM assemblages and processing such data into useful information for the network manager.[Ref. 8]

Although the CNCE is primarily programmed and configurated to operate in an Air Force environment, due to its jointness in design and development, only minor

modifications are necessary in order for it to be utilized in an Army tactical communications network.

B. THE MITRE SOLUTION

The MITRE corporation is a government-contracted establishment that performs research and development on numerous military projects. Engineers have prototyped a telemetry processing capability that focused on hardware and software modifications to demonstrate the technical feasibility of intercepting and processing the telemetry data within a typical CSCE configuration. Considerable emphasis was placed on the current DOW system as the focal point for telemetry generation.

1. Hardware

The primary objective of the hardware design was to successfully capture the telemetry data into a PC-usable format within the CSCE. To achieve this, it is necessary to have a serial interface board that has the crude capability to capture raw binary data without respect to framing or other synchronization data. A commercial off-the-shelf synchronous card was selected that required minimal modification to implement the required capability. Modifications included placing the serial controller chip (SCC) on a jumper and looping back the Request To Send (RTS) signal output to an external synchronization pin input, which was not otherwise extended to an external interface. By so doing, the capability was then available to force the card into synchronization by forcing the RTS (active low) from a high to low state.[Ref. 4]

An additional piece of hardware was also required to convert the balanced output signals of the OCU-III to an RS-232 compatible signal. The OCU-III outputs a direct current (DC) offset balanced signal with one balanced lead providing a positive logic output (approximately 0.3V low, 4.5V high) and the other a negative logic output (0.3V high, 4.5V low). An active cable was designed and fabricated to convert the positive logic output of the OCU-III to RS-232 levels (approximately -8V high, +8V low). The active cable used an RS-232 line driver chip that was capable of being powered by the PC RS-232 data terminal ready (DTR) output (5V) through the use of a charge pump and inverting circuit.[Ref. 4]

2. Software

MITRE's software design includes the capability to bit demultiplex the 16 kbps telemetry data stream, frame and synchronize the two kbps DOWs, and character demultiplex the two kbps DOWs into individual channels. From here, the software then parses the block-oriented telemetry data into a format that is usable for the network manager.[Ref. 4]

For ease of implementation, the data received from the transmission assemblages is arranged into a column and row format based on the assemblages' respective locations within the 16 kbps telemetry data stream and channel wise within the two kbps DOW. To properly determine the DOW number, i.e., which input of the DCM the two kbps DOW was patched to at the top-of-the-hill TRC-138, the software first identifies the two kbps overhead data stream. This is accomplished by locating the overhead bit sequence of

00010001, or any other bit shifted equivalent (e.g., 00100010, 10001000), from the bit demultiplexed data. Once the overhead data stream is identified, then each subsequent two kbps DOW is assigned the identification numbers one through seven.[Ref. 4]

After the DOW number of each two kbps DOW is identified, the row position of each transmission assemblage is determined based on its character multiplexed position within the two kbps DOW. This location is uniquely identified by its relative offset from a two byte synchronization pattern (ASCII SYNC SYNC, 16 hex 16 hex) which is embedded within the two kbps DOW. This means that the first demultiplexed character following the synchronization pattern is channel 1, while the 13th character is channel 13.[Ref. 4]

After the location of each transmission assemblage on the user interface screen is established, it is represented on screen by an icon. The color of the icon is determined by the status of the assemblage: green, yellow, red, or gray. Also, additional information is conveyed based upon whether the icon is flashing or not, namely that the assemblage has changed in status. The color green is a visual indication that the shelter does not have any errors to report. The color yellow, which is only represented for the TRC-170, indicates that the TRC-170 has exceeded a BER threshold. For example, if the BER within the shelter has deteriorated to 10^{-5} and consequently has exceeded the BER threshold which is set at 10^{-7}, then a marginal BER message would be generated and the icon would turn yellow. This is meant to provide a proactive capability to identify system problems before they actually result in a loss of service. If an icon is red, then the represented shelter has

one or more error messages to report. To determine the actual error messages, the network manager has to simply place the mouse or cursor over the desired assemblage icon and either click the mouse or press the "Enter" key. After doing so, a dialogue box will appear with the corresponding assemblage errors. This is a useful approach to abstract the level of information presented to the network manager at any one time, yet provides the capability to "drill down" in order to reveal the detailed errors. The last state, represented by the color gray, is not a state formally represented by the telemetry data. It is determined through software and indicates the condition when a transmission assemblage was previously reporting telemetry data but has since ceased to do so. This could be indicative of several conditions and is useful information for the network manager.[Ref. 4]

3. Implementation

Using the nodal view of a network in Figure 2 of Chapter 2, the corresponding view of the network from the telemetry prototype would be as in Figure 6. Currently, each icon would be green, indicating that there are no errors to report within the network. Using Figure 3 of Chapter 2, an unknown event has occurred within the network where the CSCE and the TTC-39 switch have indicated that a DTG to another circuit switch is out-of-service. The nodal network manager would observe a screen as illustrated in Figure 7, where several of the icons have changed to the color red and are flashing. By systematically clicking on each icon, the errors may be observed within each shelter. The nodal manager proceeds from the assemblages closest to the node, a series of errors that

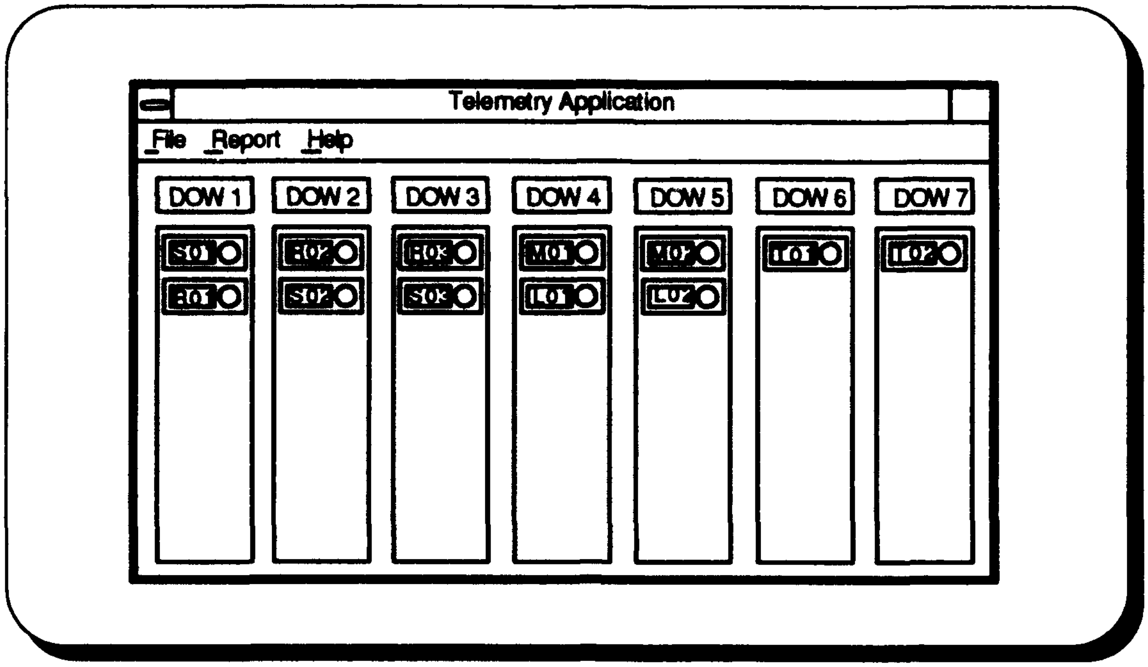

Figure 6: Transmission Network Status (No Errors)

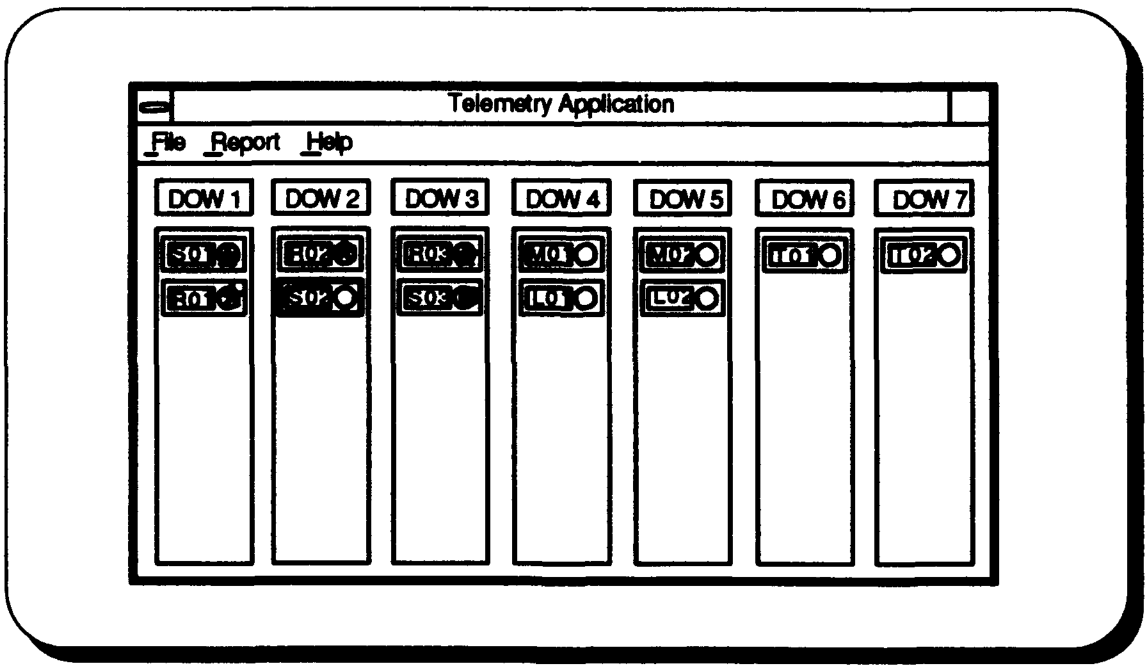

Figure 7: Transmission Network Status (System Errors)

happen to be the propagation of the original error throughout the system will be observed. Finally, after clicking on the icon for the assemblage R03 as in Figure 8, a specific error is recognized by the nodal manager as the source of the system failure. Assemblage R03 has lost receive signal from assemblage S03. This is verified by clicking on assemblage S03 which is now represented by a gray icon. At this point, the nodal network manager has specifically isolated the source of the failure. This has been accomplished within a matter of a few seconds - as long as it takes to click the mouse over each icon. Having isolated the source of the failure, the extensive time performing loopback procedures can be eliminated, and efforts focused immediately on restoring the system.[Ref. 4]

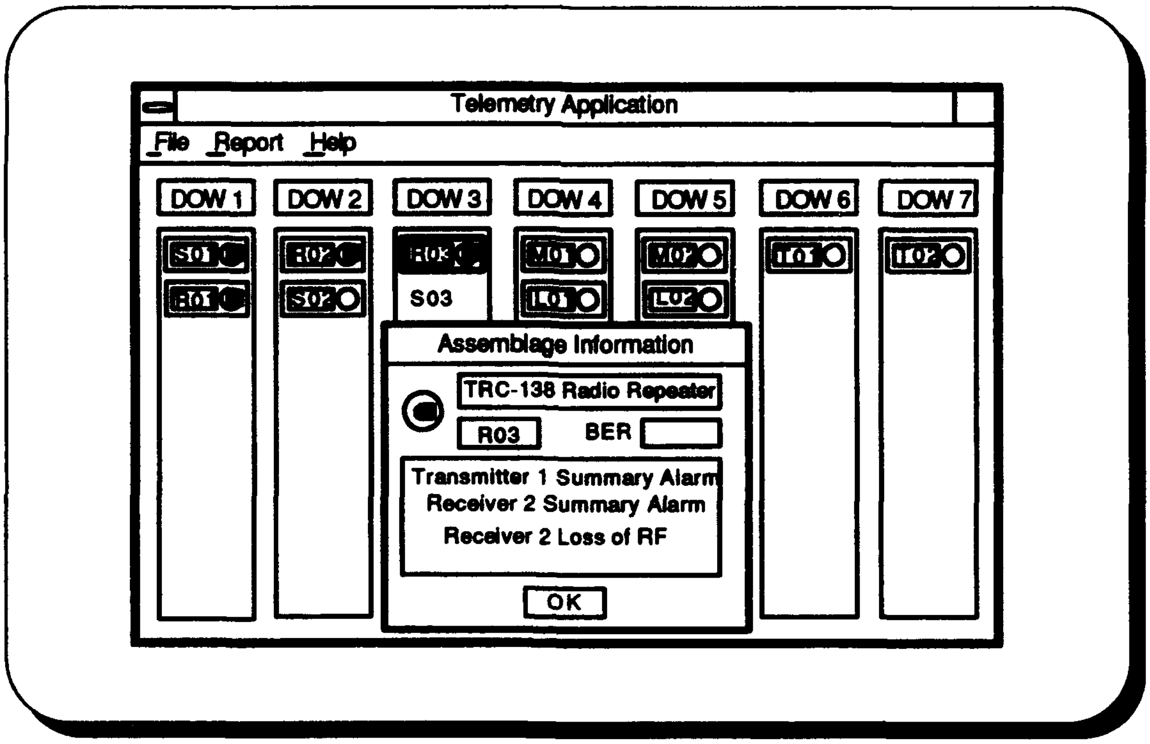

Figure 8: Isolation of System Error

C. COMMERCIAL APPLICATIONS

Another approach that is not ready for direct implementation but should be given us consideration is that of Simple Network Management Protocol (SNMP). SNMP was developed in the late 1980s to help manage the Internet and has become a de facto standard for network management. With hardware and software modifications, it could be adapted to military networks and provide capabilities that were once viewed as impossible.

In theory, SNMP allows a management station that speaks SNMP to monitor and control any network device or computer that understands SNMP. It requires three pieces of software: one for the administrator (network-management software), and two for each device you want to manage (an agent and a management information base, or MIB). Agents are pieces of software that run at each network device. They fetch information stored in the MIB database.[Ref. 9]

The administrator monitors a network by periodically polling each device and taking action if there's a problem. Some stations simply test reachability; for example, to see if the device is still up and running. Other stations can make more sophisticated queries, checking error rates, throughput, and other significant indicators of network health.[Ref. 9]

Currently, there are three standard operations that SNMP provides to allow the administrator to manipulate the network: GET, SET, and TRAP operations. A GET operation will retrieve information from the MIB about its agent, such as type of hardware/software connection. Depending upon the sophistication of the management

station, bits of information about different network devices may be requested separately or it may be possible to issue many requests at once. Likewise, the way the information is displayed and interpreted will depend on the software management station. SET operations allow the administrator to actually control the agents to some extend. For example, a manager might remotely SET the sysLocation variable on a particular system so that other managers can later request that variable to find out where the system is located. TRAPS are event notifications sent by a network device's agent to the management station. They help managers to keep an eye on the network without constantly asking every device for status information. An example of a TRAP operation is the ColdStart, which a router's agent sends out every time the router boots up. The TRAP might trigger some other action, such as downloading device-configuration information.[Ref. 9]

SNMP has the flexibility to run over various protocols and can interface with many platforms. A second version, known as SNMP2, has a master-agent/subagent architecture that allows an agent on a remote device or server to poll subagents running on subordinate devices or components. This extends the reach of management systems and helps limit polling traffic on the network. SNMP2 also resolved some of the security issues that made the original version less attractive[Ref. 10].

V. RECOMMENDATIONS

The previous chapter provided several methods of installing automated telemetry capabilities in a tactical communications network. This chapter gives a recommendation on the most efficient approach to providing such capabilities while addressing such issues as cost, security, and expandability. The chapter concludes with suggestions for future research in network telemetry.

A. RECOMMENDED APPROACH

The induction of digital communications in military applications has vastly expanded the possibilities of using telemetry to monitor tactical networks. As with the DGM equipment, most digital components have the capability of generating some form of telemetry information. A method is needed for processing such information. Since the Army has already purchased and fielded the AN/TYQ-31 (CSCE), the MITRE model is the recommended approach for implementing telemetry processing capabilities.

1. Cost

The AN/TSQ-111 shelter currently performs telemetry processing that could effectively satisfy the Army's network management requirements. It is already primed for operating in a joint environment composed of many types of equipment. As a result, the interface with Army communication shelters would not require extensive modifications to the assemblage or the network. However, due to the shrinkage in defense modernization dollars, the TSQ-111 becomes an unattractive option. It has a price tag of approximately $3.5M, excluding the cost for modifications.

The MITRE solution requires a standard PC. The software application that provides the network managers with the system status and query capabilities is government-owned, so there is no additional expense to contract software products. A processor board required to accept the raw telemetry data and convert it into usable information is estimated to cost between $260.00 and $300.00. A cable is required to connect the OCU inside the CSCE to the PC. Such cable can be fabricated by military electronic maintenance facilities or purchased at local electronic stores for a price of approximately $80.00. The final cost for providing telemetry processing to the CSCE is reportedly $360.00. Since the Army has already purchased and fielded the AN/TYQ-31 (CSCE), the MITRE solution is highly recommended.[Ref. 4]

2. Security

In the area of communications, security of information is always a vital issue. During the development phase of DGM equipment, it was determined by a study group that telemetry data should be classified information and, therefore, must be encrypted for transmission. All transmission assemblages were configured to transmit only encrypted telemetry. However, the security issue was one of the reasons the Army decided to abort telemetry usage in 1982 based on extensive hardware requirements. A secure transmission requires an encryption/decryption device at both ends. The telemetry must be decrypted at the CSCE before it can be processed. Assuming a typical node of 8-12 links (systems), this means that a CSCE would require 8-12 Dedicated Loop Encryption Devices (DLEDs) or Loop Key Generators (LKGs) to handle such a task. (Note that DGM equipment does

not use traffic channels multiplexed within groups to provide orderwires. Rather, the orderwires are frequency or time multiplexed along with the DTG. Therefore, the TED can not be used to secure the telemetry data.)

Perhaps the view of system telemetry as classified information should be reevaluated. Considering that it is the state of the network that would be in the clear, how much damage, if any, could be imposed if such information fell into the wrong hands? The telemetry is generated as raw data and would have to be transformed into meaningful information.

This thesis does not attempt to validate the need for secure telemetry. If there is a requirement, several options are available. It is possible for the CSCE to be equipped with a single DLED or LKG that performs time sharing among the 8-12 links. With the use of specialized software and hardware, the 2 kbps telemetry bit streams could be extracted from the 16 kbps ports on the OCU and presented in a logical sequence to the DLED or LKG.

3. Expandability

Realizing that what is considered "high-tech" today will be viewed as "outdated" tomorrow, it is important to adapt an approach that allows for expansion. Because of its flexibility in terms of software application, the MITRE model provides for expandability using some of the tools of Simple Network Management Protocol (SNMP) management packages. Such packages would allow the managers to create telemetry network overlays that replicate the actual network connectivity. The front end graphical user interface

(GUI) could then be used to provide changes in the network status through the use of blinking icons that symbolize the assemblages and components.[Ref. 4]

Other areas of expandability include the capability to not only monitor the network, but to actually control and reconfigure the components from a remote position. Through the use of management information bases (MIBs) inside each assemblage, the network managers could bring a backup stack or component on-line when failures occur in the primary system.

B. SUGGESTIONS FOR FURTHER RESEARCH

Although data generation capabilities currently exist, there is still issues to be expounded upon. Telemetry data is transmitted over the RF transmission media. If a transmission link goes down, telemetry messages fro the distant-end radio cannot be received by the CSCE. In addition, the radio residuals cannot be currently transmitted as part of the telemetry packet. A method for determining the cause of failure in such cases would be required utilizing a process-of-elimination matrix.

Furthermore, the DGM assemblages are currently configurated to report the status of hardware boxes and not the status of the individual DTG. A process is needed to distinguish separate DTGs within a component since one hardware box can process several DTGs.

As mentioned earlier, further research could also include a study on the impact of transmitting "unsecured" network telemetry and the implementation techniques for reconfiguring networks from a remote location.

VI. SUMMARY AND CONCLUSION

A. SUMMARY

This thesis has used a DGM tactical network model to demonstrate the feasibility and use of automated telemetry processing capabilities for reporting the "health and welfare" of a battlefield telephone system. Our current semi-manual method of residual reporting allows for erroneous and delayed information that often leads to extensive troubleshooting procedures and system downtime.

A prototype management model developed by the MITRE corporation has been recommended as an economical and viable approach to implementing generated telemetry techniques into military applications. This management system illustrates that from one central location, communication commanders and network managers can receive real-time network status updates down to the component level. In addition, the software applications of the MITRE model make it adaptable to commercial off-the-shelf developments that could further expand the network management platform.

B. CONCLUSION

This thesis has validated that a self-monitoring tactical network is possible to implement using current equipment assigned to Army signal units. Its intent is to bring to the forefront a hidden gem that could vastly improve the way tactical networks are managed. Statistics show that the CSCE assemblage that was developed to enhance network management is routinely not deployed with tactical units due to its inability to process telemetry data.

As we prepare for the 21st century, the equipment that we use to install networks will become more technical and sophisticated while the force that is responsible for its operation will, in all probability, continue to shrink. Through the use of telemetry in tactical networks, it is conceivable to product unmanned communication shelters with little or no operator intervention.

The concept of telemetry processing through automation, as provided by current and future technology, will greatly enhance the quality of communication support to the fighting forces of the Army and the Department of Defense.

APPENDIX A. ACRONYMS

ACUS	Area Common User System
ADT	Automatic Digital Tester
ASCII	American Standard Code for Information Interchange
AVOW	Analog Voice Orderwire
BER	Bit Error Rate
BPS	Bits per second
CNCE	Communications Nodal Control Element
CRF	Channel Reassignment Function
CS	Circuit Switch
CSCE	Communications System Control Element
DCM	Data Channel Multiplexer
DGM	Digital Group Multiplex
DIP	Dual-in-line Package
DLED	Digital Loop Encryption Device
DOW	Data Orderwire
DTG	Digital Transmission Group
DTR	Data Terminal Ready
DVOW	Digital Voice Orderwire
EAC	Echelons Above Corps
FM	Frequency Modulation
GM	Group Modem
HSCDM	High Speed Cable Driver Modem
HSPR	High Speed Pulse Restorer
ID	Identifier
KBPS	Kilobits per second
KM	Kilometers
LGM	Loop Group Multiplexer
LKG	Loop Key Generator
LOS	Line-of-sight
LSCDM	Low Speed Cable Driver Modem
LSPR	Low Speed Pulse Restorer
MGM	Master Group Multiplexer
MIB	Management Information Base
MSE	Mobile Subscriber Equipment
NRZ	Nonreturn-to-zero
OCU	Orderwire Control Unit
PCM	Pulse Code Modulation
PPP	Primary Patch Panel
RLGM	Remote Loop Group Multiplexer
RM	Radio Modem
RMC	Remote Multiplexer Combiner

RTS	Request to Send
SCC	Serial Controller Chip
SHF	Super High Frequency
SNMP	Simple Network Management Protocol
SPF	Signal Processing Facility
SRWBR	Short Range Wide Band Radio
TED	Trunk Encryption Device
TGM	Trunk Group Multiplexer
TOCU	Tropo Orderwire Control Unit
UHF	Ultra High Frequency
VDU	Visual Display Unit

APPENDIX B. TRANSMISSION TELEMETRY FORMAT

A telemetry transmission consists of a heading, a number of characters in data fields and an ending. The heading contains four characters: start of text (STX), generating equipment type (alphabetic) and generating equipment I.D. (two numeric characters). The remainder of the text is made up of fault or numerical data and end of text (ETX), if required, and an end of block (ETB). A fill character (Λ) is used to fill the blocks to 20 characters, where necessary.

- Character 1: Contains the start of text (STX) or continuation character (FF) to indicate the start of a message or character group or the start of a second, third, or fourth block in a message.

- Character 2: One of 16 possible alpha characters (see Table 4) identifying the reporting CESE by assemblage type classification, e.g., LOS radio and tropo radio.

- Characters 3 and 4: The numeric 00 to 99 identifying a particular assemblage of the general type identified by Character 2. These characters must be capable of being manually set in the transmission assemblage by the operator.

- Character 5 (Status): Alpha characters P (Green), E (Red), or K (Amber) denoting the status of the reporting assemblage. P indicates normal operation, i.e., no fault alarms and no BER above threshold. E denotes that at least one equipment within the assemblage is reporting a fault and possibly that a BER has exceeded its respective threshold as well. K indicates that in those assemblages with a BER monitoring capability, one or more of these monitors is reporting a BER that is higher than a pre-set threshold.

- Character 6 (Received Transmission Group Quality): For single radio assemblages, a numeric 0 to 9 indicating the BER exponent is always transmitted in this position. When the reporting assemblage has more than one reportable radio input, BER reports appear in Character 7 to 18 and a fill character (Λ) is present in this position.

- Characters 7 through 18: These twelve character positions contain either fill characters or one or two fault alarms or BER status codewords (up to six alphanumeric characters each).

- Character 19: Contains the end of text character (ETX) denoting the end of a message group. In the case of multi-block messages, fill characters appear in all but the last block which contains the ETX character.

- Character 20: Contains the end of block character (ETB) denoting the end of any 20 character transmission block.[Ref. 11]

Table 4: Character 2 Reporting Assemblage ID (ALPHA)

CHARACTER	MEANING	EXAMPLE
A		
B		
C		
D		
E	Hi-Cap Satellite Terminal	
F	Lo-Cap Satellite Terminal	
G	Single Channel Satellite Terminal	
H	Mobile Subscriber Central	
L	LOS Radio Terminal	AN/TRC-173
M	LOS Radio Repeater	AN/TRC-174
P	LOS Radio/D&I Facility	AN/TRC-178
R	TOH SRWBR	AN/TRC-138A
S	BOH SRWBR	AN/TRC-175
T	Tropo Radio Terminal	AN/TRC-170
X	Multiplexer Van	AN/TSQ-146

The DGM equipment will input one or all of the following alarms to the telemetry CSCE: equipment summary alarm (SA), loss of signal alarm (LS), and loss of frame sync alarm (FS). The meaning of the alarm words are given below:

OCU Generated Alarms

Alarm Word	Meaning
RCVSA 1, 2, 3	Receiver 1, 2, or 3 Summary Alarm
RCVRS 1, 2, 3	Receiver 1, 2, or 3 loss of Received Signal
MGMSA 1, 2	Master Group Multiplexer 1 or 2 Summary Alarm
MGMFS 1, 2	Master Group Multiplexer 1 or 2 Out of Frame
GMSA 1, 2, 3, 4, 5, 6	Group Modem 1, 2, 3, 4, 5, or 6 Summary Alarm
GMLS 1, 2, 3, 4, 5, 6	Group Modem 1, 2, 3, 4, 5, or 6 Loss of Signal
HCDSA 1, 2	High Speed Cable Driver 1 or 2 Summary Alarm
HCDLS 1, 2	High Speed Cable Driver 1 or 2 Loss of Signal
LCDSA 1, 2	Low Speed Cable Driver 1 or 2 Summary Alarm
LCDLS 1, 2	Low Speed Cable Driver 1 or 2 Loss of Signal
TGM 1, 2	Trunk Group Multiplexer 1 or 2 Summary Alarm
CNVSA 1, 2	Converter 1 or 2 Summary Alarm
RCDSA 1, 2	Remote Cable Driver 1 or 2 Summary Alarm
RCDLS 1, 2	Remote Cable Driver 1 or 2 Loss of Signal
XMTR 1, 2, 3	Transmitter 1, 2, or 3 Summary Alarm
OCU	Orderwire Control Unit Summary Alarm

OCU Generated Alarms (Continued)

Alarm Word	Meaning
DLED	Dedicated Loop Encryption Device Summary Alarm
TED 1, 2, 3, 4	Trunk Encryption Device 1, 2, 3, or 4 Summary
MAJOR	Major Alarm (more than 8 alarms)

LIST OF REFERENCES

1. Stallings, W., *Data and Computer Communications*, 3d ed., Macmillian Publishing Company, 1991.

2. Department of Defense, Joint and Multiservice Publication 6-05.4, *Joint Transmission System*, 1 July 1990.

3. Commander, U.S. Army Signal Center and Fort Gordon, Attention: ATZH-CDM, Fort Gordon, Georgia 30905-5000, SUBJECT: Required Operational Capabilities for the Integrated System Control, UNCLASSIFIED, 5 December 1990.

4. Knisley, J. R., and Werchan, H. A., "Telemetry: Enhancing Tactical Network Management," (Unpublished).

5. Department of Defense, Joint and Multiservice Publication 6-05.2, *Joint Voice Communications Systems* (Draft), 19 June 1992.

6. GTE Mobile Subscriber Equipment Division, 400 John Quincy Adams Road, Taunton, Massachusetts 02780, Mobile Subscriber Equipment: Commander's Brief, 1992.

7. Webster's *New Collegiate Dictionary*, G. & C. Merriam Company, 1979.

8. Department of Defense, Joint and Multiservice Publication 6-05.6, *Joint Technical Control Procedures/Systems*, 1 July 1990.

9. Snyder, J., "SNMP Revealed," *Macworld*, vol. 11, no. 2, pp. 182-187, February 1994.

10. Smalley, E., "Banyan Prepares to Roll Out SNMP2 Management Plan," *PC Week*, vol.11, no. 29, p. 6, July 1994.

11. Department of Defense, Joint Tactical Command, Control, and Communications Agency ICD No. 001A, *Interface Control Document for Voice and Data Orderwire Content and Signaling Information*, 28 August 1986.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 052 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Commander, USASC&FG Attn: ATZH-CDM (Don Jones) Ft. Gordon, GA 30905-5075	1
4.	Ted Lewis, Chairman, Code CS/Lt Department of Computer Science Naval Postgraduate School Monterey, Californai 93943-5118	1
5.	Lou Stevens, Code CS/St Department of Computer Science Naval Postgraduate School Monterey, California 93943-5002	1
6.	Computer Technology, Code 32 Naval Postgraduate School Monterey, California 93943-5002	1
7.	C. Thomas Wu, Code CS/Wq Department of Computer Science Naval Postgraduate School Monterey, California 93943-5002	1
8.	CPT Lucious B. Morton Rte, 4 Box 329A Abbeville, S.C. 29620	1